DEVICE AUTHENTICATION METHOD, SYSTEM AND AUTHENTICATION SYSTEM

Publication number: JP11008618

Publication date: 1999-01-12

Inventor: KATO TAKEHISA; ENDO NAOKI

Applicant: TOKYO SHIBAURA ELECTRIC CO

Classification:

- international: ***H04L9/32; H04L9/14;*** **H04L9/32; H04L9/14;** (IPC1-7): H04L9/32

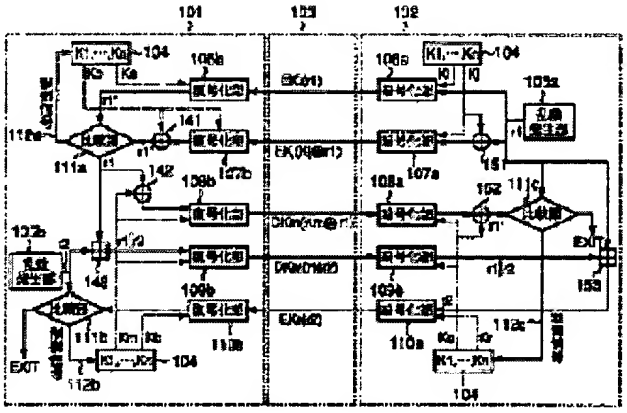
- european:

Application number: JP19970160039 19970617

Priority number(s): JP19970160039 19970617

Abstract of **JP11008618**

PROBLEM TO BE SOLVED: To allow a system to authenticate securely and surely whether or not an opposite party is a valid device by making more difficult to estimate a secret key against a 3rd party's attack. SOLUTION: The system is provided with a storage means that stores a bundle of a plurality of different private keys, a random number generating means 105a, encryption means 106a, 107a that uses a random number generated by a random number generating means or applies a prescribed arithmetic operation to the random number, uses any private key of the bundle for an encryption key to conduct encryption and to produce authentication information a communication means that sends the authentication information to a device of an authentication object, and a decoding means 108a that decodes return information received from the device of the authentication object by using the key bundle, and an authentication means 111c that compares decoding information r1' decoded by the decoding means with a random number r1 and authenticates the device of the authentication object to be a legal device when the docoded information is based on the random number.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－8618

(43)公開日　平成11年(1999)1月12日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ａ

審査請求　未請求　請求項の数17　ＯＬ　（全 17 頁）

(21)出願番号　特願平9－160039

(22)出願日　平成９年(1997)６月17日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　加藤　岳久
東京都府中市東芝町１番地　株式会社東芝府中工場内

(72)発明者　遠藤　直樹
東京都府中市東芝町１番地　株式会社東芝府中工場内

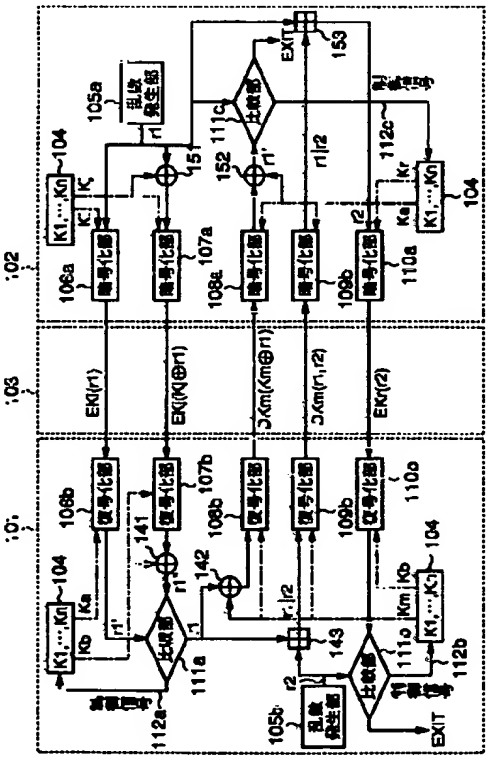
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　機器認証方法及び装置並びに認証システム

(57)【要約】

【課題】　本発明は、第三者の攻撃による秘密鍵の推定を一層困難にし、相手が正当な機器であるかを安全かつ確実に認証できる。

【解決手段】　複数の異なる秘密鍵からなる鍵束を格納する記憶手段２３と、乱数発生手段１０５ａと、乱数発生手段により発生された乱数をそのまま又は所定の演算を施した後に、鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、認証用情報を生成する暗号化手段１０６ａ，１０７ａと、認証用情報を認証対象となる機器に送出する通信手段２１と、通信手段からの認証用情報の送出に対応して、認証対象となる機器から受信した返信情報を鍵束を用いて復号化する復号化手段１０８ａと、復号化手段により復号化された復号情報ｒ１´と、乱数ｒ１とを比較し、復号情報が乱数に基づくものである場合には、認証対象となる機器は正当な機器であると認証する認証手段１１１ｃとを備えた機器認証装置。



【特許請求の範囲】

【請求項1】　複数の異なる秘密鍵からなる鍵束を格納する記憶手段と、
乱数発生手段と、
前記乱数発生手段により発生された乱数をそのまま又は所定の演算を施した後に、前記鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、認証用情報を生成する暗号化手段と、
前記認証用情報を認証対象となる機器に送出する通信手段と、
前記通信手段からの認証用情報の送出に対応して、前記認証対象となる機器から受信した返信情報を前記鍵束を用いて復号化する復号化手段と、
前記復号化手段により復号化された復号情報と、前記乱数とを比較し、前記復号情報が前記乱数に基づくものである場合には、前記認証対象となる機器は正当な機器であると認証する認証手段とを備えたことを特徴とする機器認証装置。

【請求項2】　前記暗号化手段は、前記暗号鍵として前記鍵束のうちの複数の秘密鍵を使用して、夫々の暗号鍵に対応した暗号化を行い、
前記通信手段は、前記暗号化手段で得られる各認証用情報のすべてを認証用情報として送出することを特徴とする請求項1記載の機器認証装置。

【請求項3】　前記認証対象となる機器から前記返信情報とともに相互認証用情報を受信した場合に、前記相互認証用情報を前記鍵束を用いて復号化して、原相互認証用情報を取り出す第2の復号化手段と、
前記対象となる機器が正当な機器であると認証された場合に、前記原相互認証用情報そのまま又はこれに所定の演算を施した後に、前記鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、第2の返信情報を生成する第2の暗号化手段とを備え、
前記通信手段は前記第2の返信情報を送出することを特徴とする請求項1又は2記載の機器認証装置。

【請求項4】　複数の異なる秘密鍵からなる鍵束を格納する記憶手段と、
認証を求める機器から受信した認証用情報を、前記鍵束の秘密鍵の何れかを復号鍵として復号し、又は前記復号鍵で復号するとともに所定の演算を施して、原認証用情報を取り出す復号化手段と、
前記原認証用情報をそのまま又は所定の演算を施した後に、前記鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、返信情報を生成する暗号化手段と、
前記返信情報を前記認証を求める機器に返信する通信手段とを備えたことを特徴とする機器認証装置。

【請求項5】　前記認証を求める機器から受信した認証用情報が複数の認証用情報からなるとき、夫々何れかの復号鍵で前記復号化手段により夫々取り出された複数の原認証用情報を比較し、これらの原認証用情報が一致するときには当該原認証用情報を最終的な原認証用情報として認定し、一致しないときには復号に用いる復号鍵を変更して再度復号を行うように前記復号化手段に指令する比較手段を備えたことを特徴とする請求項4記載の機器認証装置。

【請求項6】　乱数発生手段と、
前記原認証用情報と前記乱数発生手段から生成した乱数とを用いた所定の演算を行うとともに、前記鍵束のうち何れかの秘密鍵を暗号鍵として暗号化を行い、相互認証用情報を生成する第2の暗号化手段と、
前記通信手段は、前記返信情報とともに前記相互認証用情報をも送出し、
前記相互認証用情報に対する前記認証を求める機器からの第2の返信情報を前記鍵束を用いて復号化する第2の復号化手段と、
前記第2の復号化手段により復号化された復号情報と、前記乱数とを比較し、前記復号情報が前記乱数に基づくものである場合には、前記認証対象となる機器は正当な機器であると認証する認証手段とを備えたことを特徴とする請求項4又は5記載の機器認証装置。

【請求項7】　請求項1記載の機器認証装置を有する一方の機器と、
請求項4記載の機器認証装置を有する他方の機器とを備えるとともに、かつ各機器認証装置の前記鍵束の秘密鍵の少なくとも1つ以上が一致しており、前記一方の機器が前記他方の機器を正当な機器であるか否かを判定することを特徴とする認証システム。

【請求項8】　請求項2記載の機器認証装置を有する一方の機器と、
請求項5記載の機器認証装置を有する他方の機器とを備えるとともに、かつ各機器認証装置の前記鍵束の秘密鍵の少なくとも2つ以上が一致しており、前記一方の機器が前記他方の機器を正当な機器であるか否かを判定することを特徴とする認証システム。

【請求項9】　請求項3記載の機器認証装置を有する一方の機器と、
請求項6記載の機器認証装置を有する他方の機器とを備えるとともに、かつ各機器認証装置の前記鍵束の秘密鍵の少なくとも2つ以上が一致しており、前記一方の機器と前記他方の機器とで相互に認証を行うことを特徴とする相互認証システム。

【請求項10】　前記暗号化手段は2つの暗号鍵を使用するとともに、前記鍵束の秘密鍵の数がn、各暗号鍵の番号をそれぞれi，jとするときに、j＝（i＋c）mod　n（cは定数、1≦c＜n）の関係を有することを特徴とする請求項2又は3記載の機器認証装置。

【請求項11】　前記復号化手段は2つの復号鍵を使用するとともに、前記鍵束の秘密鍵の数がn、各復号鍵の番号をそれぞれi，jとするときに、j＝（i＋c）mod　n（cは定数、1≦c＜n）の関係を有すること

を特徴とする請求項５又は６記載の機器認証装置。
【請求項１２】　前記各機器認証装置の前記鍵束が同一であって、前記復号化手段は２つの復号鍵を使用するとともに、請求項３記載の機器認証装置の第２の暗号化手段に用いる暗号鍵の番号をｉと、請求項６記載の機器認証装置の第２の暗号化手段に用いる暗号鍵の番号をｊとし、前記鍵束の秘密鍵の数がｎとするときに、ｊ＝（ｉ＋ｃ）ｍｏｄ　ｎ（ｃは定数、１≦ｃ＜ｎ）の関係を有することを特徴とする請求項９の相互認証システム。
【請求項１３】　前記各機器認証装置の前記鍵束が同一であって、前記復号化手段は２つの復号鍵を使用するとともに、
請求項３記載の機器認証装置の暗号化手段に用いる複数の暗号鍵が同一の秘密鍵であり、かつ請求項６記載の機器認証装置の復号化手段に用いる複数の復号鍵が同一の秘密鍵であって、
かつ請求項３記載の機器認証装置の第２の暗号化手段に用いる暗号鍵と、請求項６記載の機器認証装置の第２の暗号化手段に用いる暗号鍵が同一であることを特徴とする請求項９の相互認証システム。
【請求項１４】　前記暗号化手段及び又は前記第２の暗号化手段は、一の暗号鍵による同一の暗号化を、各暗号化対象について選択的にあるいはすべての暗号化対象について、２回以上繰り返すことを特徴とする請求項１乃至３のうち何れか１項記載の機器認証装置。
【請求項１５】　前記復号化手段及び又は前記第２の復号化手段は、一の復号鍵による同一の復号化を、各復号化対象について選択的にあるいはすべての復号化対象について、２回以上繰り返すことを特徴とする請求項４乃至６のうち何れか１項記載の機器認証装置。
【請求項１６】　第１の機器において、乱数発生手段により発生された乱数をそのまま又は所定の演算を施した後に、複数の異なる秘密鍵からなる鍵束のうち、いずれか複数の秘密鍵を暗号鍵として複数種類の暗号化を行い、これに対応して夫々認証用情報を生成する第１の暗号化ステップと、
前記認証用情報を第１の機器から第２の機器へ送出する第１の送信ステップと、
前記第２の機器において、前記第１の機器から受信した複数の前記認証用情報夫々を、前記鍵束の秘密鍵の何れかを復号鍵として夫々復号し、又は前記復号鍵で夫々復号するとともに所定の演算を施して、夫々原認証用情報を取り出す第１の復号化ステップと、
取り出された各原認証用情報を比較し、これらの原認証用情報が一致するときには当該原認証用情報を最終的な原認証用情報としての前記乱数であると認定し、一致しないときには復号に用いる復号鍵を変更して再度前記第１の復号化ステップ復号をやり直す比較ステップと、
前記乱数をそのまま又は所定の演算を施した後に、前記鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、返信情報を生成する第２の暗号化ステップと、
前記返信情報を第２の機器から第１の機器へ返信する第２の送信ステップと、
前記第１の機器において、前記返信情報を前記鍵束を用いて復号化する第２の復号化ステップと、
前記第２の復号化手段により復号化された復号情報と、前記乱数とを比較し、前記復号情報が前記乱数に基づくものである場合には、前記第２の機器は正当な機器であると認証する認証ステップとを有することを特徴とする機器認証方法。
【請求項１７】　第１の機器において、乱数発生手段により発生された乱数をそのまま又は所定の演算を施した後に、複数の異なる秘密鍵からなる鍵束のうち、いずれか複数の秘密鍵を暗号鍵として複数種類の暗号化を行い、これに対応して夫々認証用情報を生成する第１の暗号化ステップと、
前記認証用情報を第１の機器から第２の機器へ送出する第１の送信ステップと、
前記第２の機器において、前記第１の機器から受信した複数の前記認証用情報夫々を、前記鍵束の秘密鍵の何れかを復号鍵として夫々復号し、又は前記復号鍵で夫々復号するとともに所定の演算を施して、夫々原認証用情報を取り出す第１の復号化ステップと、
取り出された各原認証用情報を比較し、これらの原認証用情報が一致するときには当該原認証用情報を最終的な原認証用情報としての前記乱数であると認定し、一致しないときには復号に用いる復号鍵を変更して再度前記第１の復号化ステップ復号をやり直す比較ステップと、
前記乱数をそのまま又は所定の演算を施した後に、前記鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、返信情報を生成する第２の暗号化ステップと、
前記乱数と第２の乱数とを用いた所定の演算を行うとともに、前記鍵束のうち何れかの秘密鍵を暗号鍵として暗号化を行い、相互認証用情報を生成する第３の暗号化手段と、
前記返信情報及び前記相互認証用情報を前記第２の機器から前記第１の機器へ返信する第２の送信ステップと、
前記第１の機器において、前記返信情報を前記鍵束を用いて復号化する第２の復号化ステップと、
前記第２の復号化手段により復号化された復号情報と、前記乱数とを比較し、前記復号情報が前記乱数に基づくものである場合には、前記第２の機器は正当な機器であると認証する第１の認証ステップと、
前記相互認証用情報を前記鍵束を用いて復号化し、さらに所定の演算を施して前記第２の乱数を取り出す第３の復号化ステップと、
前記第２の機器が正当な機器であると認証された場合に、前記第２の乱数そのまま又はこれに所定の演算を施した後に、前記鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、第２の返信情報を生成する第４の暗

号化ステップと、
前記第２の返信情報を前記第１の機器から前記第２の機器へ返信する第３の送信ステップと、
前記第１の機器からの前記第２の返信情報を前記鍵束を用いて復号化する第４の復号化手段と、
前記第４の復号化手段により復号化された復号情報と、前記第２の乱数とを比較し、前記復号情報が前記第２の乱数に基づくものである場合には、前記第１の機器は正当な機器であると認証する第２の認証ステップとを有することを特徴とする機器相互認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワーク等のデータ伝送手段を介して相手が正当な機器であるかどうか認証をする機器認証方法及び装置方法並びに認証システムに関するものである。
【０００２】
【従来の技術】最近は、マルチメディアの発展に伴つて機器のネットワーク化が進み、パーソナルコンピュータ等の汎用計算機間のみならず、オーディオ機器やビデオ機器等のオーディオヴィジュアル機器（ＡＶ機器）とのデータの送受信、ケーブルテレビや衛生放送のディジタル化等、データのディジタル化、ネットワーク化が一般的になりつつある。
【０００３】そこで、コンピュータとＡＶ機器等のディジタル機器との間でデータの送受信を行うためのディジタルインターフェース方式の統一規格が検討されている。その中の一つにＩＥＥＥ１３９４がある。ＩＥＥＥ１３９４は、１００Ｍｂｐｓ，２００Ｍｂｐｓまた４００Ｍｂｐｓ等の高転送速度を規定する規格で、この他にウルトラＳＣＳＩやＵＳＢ等の高転送速度のインターフェースが次々と規定されている。
【０００４】一方、近年ディジタル記録再生機器の開発、製品化が進み、画質や音質の劣化なくデータをコピーすることが可能となっている。したがって、これらのディジタル記録再生機器と上記高速度データ転送を扱う規格を組み合わせれば、映像データ等の大容量のデータであっても高画質な複製等を容易に実行できる。
【０００５】しかし高画質な複製は、海賊版と呼ばれる不正なコピーを増加させ、著作権が侵害されるという問題がある。このような不正なコピーは確実に防止されなければならない。というのも、インターネットやディジタルＶＴＲやＤＶＤ－ＲＡＭの出現により、ディジタル化された著作物は簡単にコピーされ、不特定多数への配布が可能となり、これによりディジタル画像の著作権者に危機感を与えているからである。
【０００６】不正コピーを行う手段としては種々の方法が考えられるが、とにかく不正者は例えばＤＶＤ－ＲＯＭドライブといった再生装置等の機器からコピー対象とするデータを受け取らなければならない。このデータ受取経路としては、機器間の通信線を介する受け取り、インターネットや公衆回線網等を介するネットワーク通信による受け取り、またコンピュータのＣＰＵバス等を介する受け取り等の経路がある。不正者はこれらの経路から一見通常の動作をする不正な機構を備えた機器、例えばＭＰＥＧ２デコータ等で正常なデータ復号をしつつ、そのオリジナルデータを横流しすること等が考えられる。
【０００７】したがって、上記のいずれの経路を介するにせよ、海賊行為を行うための不正な機器にデータを送らないようにすれば、上記不正コピーを防止することができる。
【０００８】このため、従来から、機器間でデータ送信にあたり機器の相互認証を行い、送信相手が正当な機器であることを確認してからデータ送出を行う技術が用いられている。
【０００９】このような通信機器間で相互認証するための技術として、公開鍵暗号方式とディジタル署名を組み合せた方式と、共通鍵暗号方式を用いたチャレンジ・アンド・レスポンス方式などがある。
【００１０】このうち公開鍵暗号方式は、例えば第三者機関による公開鍵証明を行い、証明書を発行する機関が必要となるため扱いが繁雑であり、また、一般的に暗号化／復号化に要する時間がかかる。
【００１１】そこで、上記したような状況では、チャレンジ・アンド・レスポンス方式が用いられることが多い。チャレンジ・アンド・レスポンス方式では、送信側と受信側で共通する秘密カギ（共通鍵）、キー＊１を持っている。ここでまず、送信側が乱数生成しこれを受信側に転送る。受信側ではこの乱数とキー＊１を用いてチャレンジキーと呼ばれるキーを作り、送信側に転送する。送信側では、最初の乱数と自己が有するキー＊１を用いてチャレンジキーに相当する比較用キーを作り、この比較用キーと受信側から受け取ったチャレンジキーが一致していれば受信側を正当な機器として認証する。次に、これと同様な認証作業が受信側から送信側に対して行われ、送信側も正当な機器であれば相互認証が成立する。
【００１２】
【発明が解決しようとする課題】しかしながら、チャレンジ・アンド・レスポンス方式等の共通鍵暗号方式では、共通鍵が漏洩した場合セキュリティが保てなくなるという問題がある。また、単に乱数を送って共通鍵で確認し合うというだけでは、真に正当な相手であるか否かを評価確認するには不十分であり、より確実安全な認証方法が従来から求められていた。
【００１３】本発明は、このような実情を考慮してなされたもので、第三者の攻撃による秘密鍵の推定を一層困難にし、相手が正当な機器であるかを安全かつ確実に認証できる機器認証方法及び装置並びに認証システムを提

供することを目的とする。

【0014】

【課題を解決するための手段】本発明の骨子は、共通鍵を複数個使用し、かつ鍵及び乱数を用いた暗号化あるいは復号化の演算を施してから認証用情報を送出することで、第三者の攻撃による秘密鍵の推定を一層困難にし、より安全に相手が正当な機器であるかを認証できることにある。

【0015】また、上記課題の解決は、より具体的には、以下のような解決手段により実現される。まず、請求項1に対応する発明は、複数の異なる秘密鍵からなる鍵束を格納する記憶手段と、乱数発生手段と、乱数発生手段により発生された乱数をそのまま又は所定の演算を施した後に、鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、認証用情報を生成する暗号化手段と、認証用情報を認証対象となる機器に送出する通信手段と、通信手段からの認証用情報の送出に対応して、認証対象となる機器から受信した返信情報を鍵束を用いて復号化する復号化手段と、復号化手段により復号化された復号情報と、乱数とを比較し、復号情報が乱数に基づくものである場合には、認証対象となる機器は正当な機器であると認証する認証手段とを備えた機器認証装置である。

【0016】次に、請求項2に対応する発明は、請求項1に対応する発明において、暗号化手段は、暗号鍵として鍵束のうちの複数の秘密鍵を使用して、夫々の暗号鍵に対応した暗号化を行い、通信手段は、暗号化手段で得られる各認証用情報のすべてを認証用情報として送出する機器認証装置である。

【0017】また、請求項3に対応する発明は、請求項1又は2に対応する発明において、認証対象となる機器から返信情報とともに相互認証用情報を受信した場合に、相互認証用情報を鍵束を用いて復号化して、原相互認証用情報を取り出す第2の復号化手段と、対象となる機器が正当な機器であると認証された場合に、原相互認証用情報そのまま又はこれに所定の演算を施した後に、鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、第2の返信情報を生成する第2の暗号化手段とを備え、通信手段は前記第2の返信情報を送出する機器認証装置である。

【0018】さらに、請求項4に対応する発明は、複数の異なる秘密鍵からなる鍵束を格納する記憶手段と、認証を求める機器から受信した認証用情報を、鍵束の秘密鍵の何れかを復号鍵として復号し、又は復号鍵で復号するとともに所定の演算を施して、原認証用情報を取り出す復号化手段と、原認証用情報をそのまま又は所定の演算を施した後に、鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、返信情報を生成する暗号化手段と、返信情報を前記認証を求める機器に返信する通信手段とを備えた機器認証装置である。

【0019】さらにまた、請求項5に対応する発明は、請求項4に対応する発明において、認証を求める機器から受信した認証用情報が複数の認証用情報からなるとき、夫々何れかの復号鍵で復号化手段により夫々取り出された複数の原認証用情報を比較し、これらの原認証用情報が一致するときには当該原認証用情報を最終的な原認証用情報として認定し、一致しないときには復号に用いる復号鍵を変更して再度復号を行うように復号化手段に指令する比較手段を備えた機器認証装置である。

【0020】一方、請求項6に対応する発明は、請求項4又は5に対応する発明において、乱数発生手段と、原認証用情報と乱数発生手段から生成した乱数とを用いた所定の演算を行うとともに、鍵束のうち何れかの秘密鍵を暗号鍵として暗号化を行い、相互認証用情報を生成する第2の暗号化手段と、通信手段は、返信情報とともに相互認証用情報をも送出し、相互認証用情報に対する認証を求める機器からの第2の返信情報を鍵束を用いて復号化する第2の復号化手段と、第2の復号化手段により復号化された復号情報と、乱数とを比較し、復号情報が乱数に基づくものである場合には、認証対象となる機器は正当な機器であると認証する認証手段とを備えた機器認証装置である。

【0021】次に、請求項7に対応する発明は、請求項1記載の機器認証装置を有する一方の機器と、請求項4記載の機器認証装置を有する他方の機器とを備えるとともに、かつ各機器認証装置の鍵束の秘密鍵の少なくとも1つ以上が一致しており、一方の機器が他方の機器を正当な機器であるか否かを判定する認証システムである。

【0022】また、請求項8対応する発明は、請求項2記載の機器認証装置を有する一方の機器と、請求項5記載の機器認証装置を有する他方の機器とを備えるとともに、かつ各機器認証装置の鍵束の秘密鍵の少なくとも2つ以上が一致しており、一方の機器が他方の機器を正当な機器であるか否かを判定する認証システムである。

【0023】さらに、請求項9対応する発明は、請求項3記載の機器認証装置を有する一方の機器と、請求項6記載の機器認証装置を有する他方の機器とを備えるとともに、かつ各機器認証装置の鍵束の秘密鍵の少なくとも2つ以上が一致しており、一方の機器と他方の機器とで相互に認証を行う相互認証システムである。

【0024】さらにまた、請求項10対応する発明は、請求項2又は3に対応する発明において、暗号化手段は2つの暗号鍵を使用するとともに、鍵束の秘密鍵の数がｎ、各暗号鍵の番号をそれぞれｉ，ｊとするときに、ｊ＝（ｉ＋ｃ）ｍｏｄ　ｎ（ｃは定数、1≦ｃ＜ｎ）の関係を有する機器認証装置である。

【0025】一方、請求項11対応する発明は、請求項5又は6に対応する発明において、復号化手段は2つの復号鍵を使用するとともに、鍵束の秘密鍵の数がｎ、各復号鍵の番号をそれぞれｉ，ｊとするときに、ｊ＝（ｉ

＋ｃ）ｍｏｄ　ｎ（ｃは定数、１≦ｃ＜ｎ）の関係を有する機器認証装置である。

【００２６】また、請求項１２対応する発明は、請求項９に対応する発明において、各機器認証装置の鍵束が同一であって、復号化手段は２つの復号鍵を使用するとともに、請求項３記載の機器認証装置の第２の暗号化手段に用いる暗号鍵の番号をｉと、請求項６記載の機器認証装置の第２の暗号化手段に用いる暗号鍵の番号をｊとし、鍵束の秘密鍵の数がｎとするときに、ｊ＝（ｉ＋ｃ）ｍｏｄ　ｎ（ｃは定数、１≦ｃ＜ｎ）の関係を有する相互認証システムである。

【００２７】さらに、請求項１３対応する発明は、請求項９に対応する発明において、各機器認証装置の鍵束が同一であって、復号化手段は２つの復号鍵を使用するとともに、請求項３記載の機器認証装置の暗号化手段に用いる複数の暗号鍵が同一の秘密鍵であり、かつ請求項６記載の機器認証装置の復号化手段に用いる複数の復号鍵が同一の秘密鍵であって、かつ請求項３記載の機器認証装置の第２の暗号化手段に用いる暗号鍵と、請求項６記載の機器認証装置の第２の暗号化手段に用いる暗号鍵が同一である相互認証システムである。

【００２８】さらにまた、請求項１４対応する発明は、請求項１～３に対応する発明において、暗号化手段及び又は第２の暗号化手段は、一の暗号鍵による同一の暗号化を、各暗号化対象について選択的にあるいはすべての暗号化対象について、２回以上繰り返す機器認証装置である。

【００２９】一方、請求項１５対応する発明は、請求項４～６に対応する発明において、復号化手段及び又は第２の復号化手段は、一の復号鍵による同一の復号化を、各復号化対象について選択的にあるいはすべての復号化対象について、２回以上繰り返す機器認証装置である。

【００３０】また、請求項１６対応する発明は、第１の機器において、乱数発生手段により発生された乱数をそのまま又は所定の演算を施した後に、複数の異なる秘密鍵からなる鍵束のうち、いずれか複数の秘密鍵を暗号鍵として複数種類の暗号化を行い、これに対応して夫々認証用情報を生成する第１の暗号化ステップと、認証用情報を第１の機器から第２の機器へ送出する第１の送信ステップと、第２の機器において、第１の機器から受信した複数の認証用情報夫々を、鍵束の秘密鍵の何れかを復号鍵として夫々復号し、又は復号鍵で夫々復号するとともに所定の演算を施して、夫々原認証用情報を取り出す第１の復号化ステップと、取り出された各原認証用情報を比較し、これらの原認証用情報が一致するときには当該原認証用情報を最終的な原認証用情報としての乱数であると認定し、一致しないときには復号に用いる復号鍵を変更して再度第１の復号化ステップ復号をやり直す比較ステップと、乱数をそのまま又は所定の演算を施した後に、鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、返信情報を生成する第２の暗号化ステップと、返信情報を第２の機器から第１の機器へ返信する第２の送信ステップと、第１の機器において、返信情報を鍵束を用いて復号化する第２の復号化ステップと、第２の復号化手段により復号化された復号情報と、乱数とを比較し、復号情報が乱数に基づくものである場合には、第２の機器は正当な機器であると認証する認証ステップとを有する機器認証方法である。

【００３１】さらに、請求項１７対応する発明は、第１の機器において、乱数発生手段により発生された乱数をそのまま又は所定の演算を施した後に、複数の異なる秘密鍵からなる鍵束のうち、いずれか複数の秘密鍵を暗号鍵として複数種類の暗号化を行い、これに対応して夫々認証用情報を生成する第１の暗号化ステップと、認証用情報を第１の機器から第２の機器へ送出する第１の送信ステップと、第２の機器において、第１の機器から受信した複数の認証用情報夫々を、鍵束の秘密鍵の何れかを復号鍵として夫々復号し、又は復号鍵で夫々復号するとともに所定の演算を施して、夫々原認証用情報を取り出す第１の復号化ステップと、取り出された各原認証用情報を比較し、これらの原認証用情報が一致するときには当該原認証用情報を最終的な原認証用情報としての乱数であると認定し、一致しないときには復号に用いる復号鍵を変更して再度第１の復号化ステップ復号をやり直す比較ステップと、乱数をそのまま又は所定の演算を施した後に、鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、返信情報を生成する第２の暗号化ステップと、乱数と第２の乱数とを用いた所定の演算を行うとともに、鍵束のうち何れかの秘密鍵を暗号鍵として暗号化を行い、相互認証用情報を生成する第３の暗号化手段と、返信情報及び相互認証用情報を第２の機器から第１の機器へ返信する第２の送信ステップと、第１の機器において、返信情報を鍵束を用いて復号化する第２の復号化ステップと、第２の復号化手段により復号化された復号情報と、乱数とを比較し、復号情報が乱数に基づくものである場合には、第２の機器は正当な機器であると認証する第１の認証ステップと、相互認証用情報を鍵束を用いて復号化し、さらに所定の演算を施して第２の乱数を取り出す第３の復号化ステップと、第２の機器が正当な機器であると認証された場合に、第２の乱数そのまま又はこれに所定の演算を施した後に、鍵束のうちの何れかの秘密鍵を暗号鍵として暗号化を行い、第２の返信情報を生成する第４の暗号化ステップと、第２の返信情報を第１の機器から第２の機器へ返信する第３の送信ステップと、第１の機器からの第２の返信情報を鍵束を用いて復号化する第４の復号化手段と、第４の復号化手段により復号化された復号情報と、第２の乱数とを比較し、復号情報が第２の乱数に基づくものである場合には、第１の機器は正当な機器であると認証する第２の認証ステップとを有する機器相互認証方法である。

【００３２】
【発明の実施の形態】以下、本発明の実施の形態について説明する。
（発明の第１の実施の形態）図１は本発明の第１の実施の形態に係る機器認証方法を適用する機器の構成例を示すブロック図である。
【００３３】同図に示すように、機器認証装置を搭載した機器としてＤＶＤ－ＲＯＭドライブ１とＭＰＥＧ２デコーダ２とが１３９４ケーブル３によって接続されている。以下、ＩＥＥＥ１３９４規格に準拠した部品若しくはモジュール等を”～１３９４”又は”１３９４～”の形で表現する。
【００３４】ＤＶＤ－ＲＯＭドライブ１及びＭＰＥＧ２デコーダ２には、１３９４チップ４，５が搭載され、上記１３９４ケーブル３を介し両者間でＩＥＥＥ１３９４に従うデータ伝送がされるようになっている。
【００３５】ＤＶＤ－ＲＯＭドライブ１は、ＤＶＤ６を再生してそのデータを取り出すためのデータ再生部６と、１３９４ケーブル３を介して接続された機器の認証を行うとともに、再生されたデータを認証された機器に送出する１３９４チップ４とから構成されている。
【００３６】一方、ＭＰＥＧ２デコーダ２は、１３９４チップ５を介してＤＶＤ－ＲＯＭドライブ１から受け取ったＭＰＥＧ２圧縮されたデータを伸張し表示装置８に出力するデータ伸張部９と、１３９４ケーブル３を介して接続された機器の認証を行うとともに、ＤＶＤ－ＲＯＭドライブ１からデータ受信を行う１３９４チップ５とから構成されている。
【００３７】１３９４チップ４又は５夫々は、ＩＥＥＥ１３９４に従った通信を実行する１３９４通信部１１，２１と、鍵束格納部１２，２２と、認証部１３，２３とによって構成されている。認証部１３，２３は、鍵束格納部１２，２２に格納された鍵束を用いて接続される機器の相互認証を行うとともに、認証がされたときのみ接続機器とのデータ送受を１３９４通信部１１又は１２に許可するようになっている。なお、認証に際して必要な通信は１３９４通信部１１，２１により行われる。
【００３８】鍵束格納部１２，２２に格納された鍵束は、１３９４チップ４又は５が製造されるときに格納される秘密の情報であり、多数の秘密鍵からなっているものである。双方の鍵束は少なくとも１つの共通の鍵を有している。すなわち本実施形態の方法は共通鍵暗号方式の一種である。本実施形態では、双方の鍵束は同一のものである場合で説明する。
【００３９】ここで、本実施形態では、認証部１３、鍵束格納部１２及び１３９４通信部１１は１つのＩＣチップで構成されているが、認証部１３及び鍵束格納部１２のみで１チップとしてもよい。さらに鍵束格納部１２のみで１チップであってもよい。いずれにせよ認証部１３、鍵束格納部１２及び１３９４通信部１１の全体は、ハードウエア的には、演算手段とこれを制御するプログラムと情報を格納する記憶手段を有し、上記した各機能を実現できるようになっている。また、上記各関係は、認証部２３、鍵束格納部２２及び１３９４通信部２１についても同様である。
【００４０】次に、１３９４チップの相互認証を行う部分の構成について説明する。図２は本実施形態の相互認証を行う部分の機能構成及び処理の流れの一例を示す図である。
【００４１】同図には、主として図１の認証部１３，２３の機能的な構成が示され、これらにより認証システムが構成されている。なお、図１及び図２の対応を説明すると、１３９４チップ４が送信側１０１、１３９４チップ５が受信側１０２とされ、この間を接続する１３９４ケーブル３がネットワーク１０３として示されている。
【００４２】ここで送信側１０１は、復号化部１０６ｂ，１０７ｂ，１０８ｂ，１０９ｂ，１１０ｂと、比較部１１１ａ，１１１ｂと、乱数発生部１０５ｂと、共通鍵の鍵束１０４と、排他論理輪和演算部１４１，１４２と、連接演算部１４３とを備えている。なお、鍵束１０４は図１の鍵束格納部１２に格納されるべきものである。
【００４３】また、同様に受信側１０２は、暗号化部１０６ａ，１０７ａ，１０８ａ，１０９ａ，１１０ａと、比較部１１１ｃと、乱数発生部１０５ａと、共通鍵の鍵束１０４と、排他論理輪和演算部１５１，１５２と、連接演算部１５３とを備えている。なお、送信側と同様に、鍵束１０４は鍵束格納部２２に格納される。
【００４４】また、特にしないが図２中の送信側１０１と受信側１０２との通信は図１の１３９４通信部１１，２１によって行われる。ここで、暗号化部１０６ａと復号化部１０６ｂ、暗号化部１０７ａと復号化部１０７ｂ、暗号化部１０８ａと復号化部１０８ｂ、暗号化部１０９ａと復号化部１０９ｂ、暗号化部１１０ａと復号化部１１０ｂが対になっており、それぞれ対応するアルゴリズムで暗号化及び復号化するようになっている。これらの各暗号化部及び復号化部はそれぞれ別途に設けるようにしてもよいが、暗号又は復号アルゴリズムが同一のときには、同一の暗号手段又は復号手段を用いるようにしてもよい。
【００４５】すなわち、例えば暗号化部１０６ａ，１０７ａ，１０８ａ，１０９ａ，１１０ａによる暗号化処理は受信側１０２内の一の暗号化処理部により実行されるようにしてもよい。同様に、復号化部１０６ｂ，１０７ｂ，１０８ｂ，１０９ｂ，１１０ｂによる復号化処理は送信側１０２内の一の復号化処理部により実行されるようにしてもよい。本実施形態ではこれらは図面上異なる機能部として表現されるが、実際の処理は同一の暗号化処理部又は復号化処理部によって実行される。このようにすれば送信側１０２及び受信側１０１のハードウエア

資源及びソフトウエア資源を有効に活用することができる。

【００４６】なお本明細書では、暗号化の操作をＥｙ（ｘ）と表す。ここで、ｘは暗号化の対象となるデータで、ｙは暗号化に用いる暗号鍵である。また復号化の操作をＤｙ（ｚ）と表す。ここで、ｚは復号の対象となるデータで、ｙは復号化に用いる復号鍵である。従って、

Ｅｙ（Ｄｙ（ｘ））＝ｘ

Ｄｙ（Ｅｙ（ｘ））＝ｘ

である。

【００４７】またデータを復号化することは暗号化することと同様の効果を持つ。すなわち、Ｄｙ（ｘ）を行って結果を送信し、受信側で暗号化Ｅｙ（Ｄｙ（ｘ））を行うことと、先に暗号化して復号化することは同様の効果を持つ。厳密には暗号化のアルゴリズムと復号化のアルゴリズムは異なるものであるが、本実施形態では、便宜上、送信側１０２で行う処理を暗号化と呼び、受信側１０１で行う処理を復号化と呼んでいる。このような暗号化、復号化の順番を入れ替える理由は、上記一の暗号化処理部又は一の復号化処理部の使用により、上述したように資源の有効利用を可能とするためである。したがって、本実施形態でいう暗号化又は復号化と、特許請求の範囲でいう暗号化又は復号化は必ずしも一致しないので注意を要する。特許請求の範囲では、単に、鍵を用いて情報を暗号化する行為を暗号化といい、鍵を用いて暗号化された情報を解く行為を復号化と呼んでいる。

【００４８】また本明細書の各図において、一点鎖線は暗号化または復号化のための鍵情報を表し、実線は暗号化または復号化の対象となる情報を表している。さらに、本明細書では、排他論理輪和演算をＸＯＲ（ｘ，ｙ）、連接（ｃｏｎｃａｔｉｎａｔｉｏｎ）演算をｘ|ｙと表す。なお、図面では排他論理輪和演算を演算記号を用いて表現している。

【００４９】次に、以上のように構成された本発明の実施の形態に係る機器認証方法を適用する機器の動作について説明する。図１のＤＶＤ－ＲＯＭドライブ１からＭＰＥＧデコータ２にＤＶＤ６のデータを送出する必要が生じた場合、まず、ＤＶＤ－ＲＯＭドライブ１とＭＰＥＧデコータ２と間での相互認証の処理が実行される。

【００５０】相互認証がなされ、相互に相手が正当な機器であると確認されると、夫々の認証部１３，２３により、１３９４通信部１１，１２に通信許可が与えられる。以降、ＤＶＤ－ＲＯＭドライブ１とＭＰＥＧデコータ２とは、１３９４通信部１１，１２、１３９４ケーブル３を介して必要な通信を開始し、ＤＶＤ６のデータ転送、ＭＰＥＧ２圧縮データの伸長処理等がなされ、映像等がＣＲＴや液晶パネル等の表示装置８から表示出力される。

【００５１】ここで、図２に示す構成により１３９４チップ４，５間で上述した相互認証が行われるわけであるが、その認証処理について図２及び図３に沿って詳しく説明する。

【００５２】図３は本実施形態の認証動作例を示す流れ図である。本実施形態では、図２の受信側１０２から相互認証がスタートする場合について説明する。

【００５３】まず、受信側１０２において乱数発生部１０５ａにより、例えば時間情報などを元にして乱数が発生される。この乱数の長さは本実施形態で用いる暗号化ブロック長が望ましい。例えば、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）では６４ビットである。

【００５４】次に、ｎ個の共通鍵の鍵束１０４のうちの一つ鍵Ｋｉ（１≦ｉ≦ｎ）が選択され、乱数発生部１０５ａにより発生した乱数ｒ１は、鍵Ｋｉを暗号鍵として暗号化部１０６ａにより暗号化される。また、鍵束１０４Ｋｓ（ｓ＝１，…，ｎ；Ｋｉ≠Ｋｊ，ｉ＝１，…，ｎ，ｊ＝１，…，ｎ）というｎ個の共通鍵の鍵束のうちの一つの鍵Ｋｊ（１≦ｊ≦ｎ）が選択され、乱数ｒ１との排他論理和が排他的論理和演算部１５１にて演算されて、その結果であるＸＯＲ（Ｋｊ，ｒ１）がＫｊを暗号鍵として暗号化部１０７ａにて暗号化される。

【００５５】暗号化部１０６ａおよび１０７ａでそれぞれ暗号化されたＥＫｉ（ｒ１）およびＥＫｊ（ＸＯＲ（Ｋｊ，ｒ１））は送信側１０１へネットワーク１０３を介して伝送される（図３Ｓ１）。この伝送は、送信部１０１が受信部１０２についての認証を行うための開始処理になる。

【００５６】次に、送信側１０１では、伝送されたＥＫｉ（ｒ１）が復号化部１０６ｂにて復号される。このとき、ｎ個の共通鍵の鍵束１０４Ｋｓ（ｓ＝１，…，ｎ；Ｋｉ≠Ｋｊ，ｉ＝１，…，ｎ，ｊ＝１，…，ｎ）の中から一つの鍵Ｋａが選択され、これを復号鍵として復号化がされる。本実施形態では鍵Ｋａは、例えば鍵Ｋ１から順に選択していくものとする。復号鍵Ｋａで復号された結果をｒ１′とする。

【００５７】また、送信側１０１において、伝送されたＥＫｊ（ＸＯＲ（Ｋｊ，ｒ１））が復号化部１０７ｂにて復号される。このとき、ｎ個の共通鍵の鍵束１０４Ｋｓ（ｓ＝１，…，ｎ；Ｋｉ≠Ｋｊ，ｉ＝１，…，ｎ，ｊ＝１，…，ｎ）の中から一つの鍵Ｋｂが選択され、復号鍵として復号化がされる。本実施形態では鍵Ｋｂは、上記と同様に例えば鍵Ｋ１から順に選択していくものとする。復号化部１０７ｂで復号された結果と復号化に用いた復号鍵Ｋｂとの排他論理和を、排他的論理和演算部１４１にて計算した結果をｒ１″とする（図３Ｓ２）。

【００５８】上記各復号化部１０６ｂ，１０７ｂで得られたｒ１′とｒ１″とが比較部１１１ａにて比較される。このとき、ｒ１′≠ｒ１″であるならば、復号鍵として用いられた鍵Ｋａ，Ｋｂが違っていると判定される。このとき比較部１１１ａから制御信号１１２ａが出

力され、鍵Ka，Kb が変更されて再度復号処理がやり直される（図３Ｓ３，Ｓ４）。

【００５９】これにより、正しい鍵が見つかるまで繰り返し演算が実行される。例えばまず鍵Ka が鍵K1 に固定され、鍵Kb を鍵K1 から順に鍵Kn まで変化させる。鍵Kb が鍵Kn まで変化しても一致しなければ、鍵Ka を鍵K2 に変化させ、ふたたび鍵Kb を鍵K1 から順に鍵Kn まで変化させて復号処理を繰返し、ｒ1′とｒ1″とを比較部１１１ａにて比較する手順を繰返す。こうして、ｒ1′とｒ1″となる（すなわちKa ＝Ki，Kb ＝Kj となる）まで処理が繰返される（図３Ｓ２，Ｓ３，Ｓ４）。なお、Ka ＝Ki，Kb ＝Kj となる鍵が見つからなかった場合、ＥＸＩＴとし、認証は不成立となる（図３Ｓ４）。

【００６０】ステップＳ３において、ｒ1′＝ｒ1″となった場合、すなわちｒ1′＝ｒ1″＝ｒ1 となった場合には、送信側では１０５ｂ乱数発生部にて乱数ｒ2 を例えば時間情報を元に発生させる。この乱数の長さは本実施形態で用いる暗号化ブロック長が望ましい。例えば、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）では６４ビットである。また、ｎ個の共通鍵の鍵束１０４Ks（ｓ＝１，…，ｎ；Ki ≠Kj，ｉ＝１，…，ｎ，ｊ＝１，…，ｎ）のうちの一つである鍵Km（１≦ｍ≦ｎ）が暗号鍵として選択される。

【００６１】そして、受信側１０２で発生した乱数ｒ1 と送信側１０１で発生した乱数ｒ2の連接が連接演算部１４３にて演算され、その結果であるｒ1｜ｒ2 が鍵Km によって復号化部１０９ｂにて復号化（すなわち暗号化）される（図３Ｓ５）。

【００６２】一方、上記乱数ｒ1 と上記鍵Km との排他論理和が排他的論理和演算部１４２にて演算され、その結果であるＸＯＲ（Km，ｒ2）が鍵Km を暗号鍵として復号化部１０８ｂで復号化（すなわち暗号化）される（図３Ｓ６）。

【００６３】そして、１０８ｂおよび１０９ｂ復号化部で復号化されたＤKm（ＸＯＲ（Km，ｒ2））及びＤKm（ｒ1｜ｒ2）がネットワーク１０３を介して受信側１０２へ伝送される（図３Ｓ５，Ｓ６）。なお、ステップＳＴ６の処理は、受信部１０２からの認証要求に対する送信部１０１からの返答となっており、ステップＳＴ５の処理は、送信部１０１が受信部１０２についての認証を行うための開始処理となっている。

【００６４】次に、受信側１０２では、伝送されたＤKm（ＸＯＲ（Km，ｒ1））が暗号化部１０８ａにて暗号化される。このとき、ｎ個の共通鍵の鍵束１０４Ks（ｓ＝１，…，ｎ；Ki ≠Kj，ｉ＝１，…，ｎ，ｊ＝１，…，ｎ）の中から一つの鍵Ka が選択され、暗号鍵として暗号化される。本実施形態ではKa は、例えばＫ１から順に選択していくものとする。また、暗号鍵Ka で暗号化された結果と暗号鍵Ka との排他論理和が排他的論理和演算部１５２にて演算され、ｒ1′が得られる（図３Ｓ７）。

【００６５】得られたｒ1′と乱数発生部１０５ａで発生した乱数ｒ1 とが比較部１１１ｃにて比較される（図３Ｓ８）。このとき、ｒ1′≠ｒ1 であるならば、暗号鍵で用いた鍵Ka が違っていると判定される。これにより、比較部１１１ｃから制御信号１１２ｃが出力されて、鍵Ka が変更され再度復号処理がやり直される（図３Ｓ９）。例えば、鍵Ka を鍵K1 から順に鍵Kn まで変化させて復号処理を繰返し、ｒ1′とｒ1 とを比較部１１１ｃにて比較する手順を繰返す。こうして、ｒ1′＝ｒ1 となる（すなわちKa ＝Km となる）まで処理は繰返される（図３Ｓ７，Ｓ８，Ｓ９）。

【００６６】なお、ｍ＝ｎとなっても比較部１１１ｃによる比較においてｒ1′＝ｒ1 とならなければ、送信側は正当な鍵束Ks を所有していないとして認証手続を終了する（図３Ｓ９）。

【００６７】一方、ｒ1′＝ｒ1 となったとき、送信側１０１で用いた復号鍵Km が特定できたことになる。これは受信側１０２から見たとき送信側１０１が正当なものであると認証できたことを意味している。そこで、相互認証の処理が継続される。すなわち、まず、上記特定された鍵Km を暗号鍵としてＤKm（Km｜ｒ2）が暗号化され、ｒ1｜ｒ2 が得られる。さらに乱数発生部１０５ａで発生した乱数ｒ1 が用いられ、連接演算部１５３において送信側で発生した乱数ｒ2 が取出される（図３Ｓ１０）。

【００６８】次にｎ個の共通鍵の鍵束１０４Ks（ｓ＝１，…，ｎ；Ki ≠Kj，ｉ＝１，…，ｎ，ｊ＝１，…，ｎ）の中から一つの鍵Kr（１≦ｒ≦ｎ）が選択され、上記得られた乱数ｒ2 が鍵Kr を暗号鍵として暗号化部１１０ａにて暗号化される。そして、暗号化部１１０ａで暗号化された結果であるＥKr（ｒ2）がネットワーク１０３を介して送信側１０１へ伝送される（図３Ｓ１１）。なお、ステップＳＴ１１の処理は、送信部１０１からの認証要求に対する受信部１０２からの返答となっている。

【００６９】次に、送信側１０１では、伝送されたＥKr（ｒ2）が１１０ｂ復号化部にて復号されｒ2′が得られる。このとき、ｎ個の共通鍵の鍵束１０４Ks（ｓ＝１，…，ｎ；Ki ≠Kj，ｉ＝１，…，ｎ，ｊ＝１，…，ｎ）の中から一つの鍵Kb が選択され、これを復号鍵として復号がされる。本実施形態では鍵Kb は、例えば鍵K1 から順に選択していくものとする。

【００７０】得られたｒ2′と乱数発生部１０５ｂで発生した乱数ｒ2 とが比較部１１１ｂにて比較される。このとき、ｒ2′≠ｒ2 であるならば、暗号鍵で用いた鍵Kbが違っていると判定される。このとき、比較部１１１ｂにより制御信号１１２ｂが出力され、鍵Kb が変更されて再度復号処理がやり直される。例えば、鍵Kbが

鍵K1 から順に鍵Kn まで変化させて復号処理が繰返され、r2 ′ とr2 とを比較部１１１ｂにて比較する手順が繰返される。こうして、r2 ′ ＝r2 となる（すなわちKb ＝Kr とする）まで処理は繰返される。

【００７１】ｒ＝ｎとなってもｒ2 ′ ＝ｒ2 とならなければ、受信側１０２は正当な鍵束Ks を所有していないとして認証手続きを終了する。ｒ2 ′ ＝ｒ2 となったとき、受信側で用いた暗号鍵Kr が特定できたことになり、受信側１０２が正当な鍵束Ks を所有するとして認証する。

【００７２】以上の手順により送信側１０１、受信側１０２間での相互認証が実現される。上述したように、本発明の実施の形態に係る機器認証方法及び装置並びに認証システムは、共通鍵を複数個使用し、かつ鍵及び乱数を用いた暗号化あるいは復号化の演算を施してから認証用情報を送出するとともに、認証用情報の受け取り側でもこれに対応した復号を行って認証用情報に対する返信を行い、認証用情報の送出元で上記乱数を確認することで認証を行うようにしたので、第三者の攻撃による秘密鍵の推定を一層困難にし、より安全に相手が正当な機器であるかを認証することができる。また、認証用情報の受け取り側から認証用情報の送出元に同様な認証をかけることにより、このような安全性の高い相互認証を行うことができる。

【００７３】すなわち、複数個の共通鍵を用いて、単に乱数を暗号化して認証を行うのでなく、乱数と暗号鍵とで演算を行ない、その結果も用いることにより、暗号解読を困難にし安全性の高い相互認証が可能となる。

【００７４】また、共通鍵を複数個持ち、それらを利用するようにしたので、正当な鍵束をお互いに持っていなければ認証されない。また、鍵束とすることで、もし鍵束の秘密鍵のうちの何れかが漏洩したとしても、その漏洩した鍵を利用しないようにすればセキュリティを保つことができる。したがって、より一層の安全性を高くできるとともに、セキュリティの柔軟性をも高くすることができる。

【００７５】さらに、このような認証方式を用いたことで、また安全性をあまり落とすことなく、鍵を判定するための計算回数を減らすことが可能となる。この結果、高速な認証が可能となる。なお、計算回数を減らす具体的な方法については第２の実施形態以降で説明する。

【００７６】なお、本実施形態では、１３９４チップ４，５に別けて、一方を送信側１０１、他方を受信側１０２として説明したが、１３９４チップ４，５は送信側１０１及び受信側１０２となるべき双方の機能を備え、何れが送信側１０１又は受信側１０２となってもよいものである。

（発明の第２の実施の形態）第１の実施形態では、暗号化部１０６ａと暗号化部１０７ａとで用いられる秘密鍵Ki とKj の間に特に関係がなく、両鍵Ki とKj が任意に選択されていた。これに対し、本実施形態は秘密鍵Ki とKj との間に一定の関係を設けている。この点を除く他、本実施形態は、第１の実施形態の場合と同様に構成されている。

【００７７】すなわち本実施形態では、受信側１０２の暗号化部１０６ａと暗号化部１０７ａとでそれぞれ用いる秘密鍵Ki とKj のｉとｊとが、ｊ＝（ｉ＋ｃ）ｍｏｄｎ（ｃは定数、１≦ｃ＜ｎ）という関係を有している。また、送信側１０１でもこの関係があることを前提に、復号化部１０６ｂと復号化部１０７ｂにて復号化処理を実行する。

【００７８】上述したように、本発明の実施の形態に係る機器認証方法及び装置並びに認証システムは、第１の実施形態と同様な構成を設けた他、秘密鍵Ki とKj との間にｊ＝（ｉ＋ｃ）ｍｏｄ　ｎ（ｃは定数、１≦ｃ＜ｎ）という関係を設けたので、第１の実施形態と同様な効果が得られる他、秘密鍵Ki （Ka ）とKj （Kb）の検出には最大ｎ回の計算で済み、計算量を大幅に削減することができる。この結果、鍵判定に要する全計算量は、最大ｎ＋ｎ＋ｎ＝３ｎ回となる。

【００７９】なお、第１の実施形態で行った復号鍵Ka と復号鍵Kb の変更については、最大ｎ×ｎ回の計算が必要である。

（発明の第３の実施の形態）第１の実施形態では、秘密鍵Km とKr の間に特に関係がなく、両鍵Km とKr が任意に選択されていた。これに対し、本実施形態は秘密鍵Km とKr との間に一定の関係を設けている。この点を除く他、本実施形態は、第１の実施形態の場合と同様に構成されている。

【００８０】すなわち、復号化部１０８ｂ及び１０９ｂで用いた復号鍵Km （すなわち暗号化部１０８ａ及び１０９ａで用いる暗号鍵Km ）と、暗号化部１１０ａで用いる暗号鍵Kr のｍとｒがｒ＝（ｍ＋ｃ）ｍｏｄ　ｎ（ｃは定数、１≦ｃ＜ｎ）の関係を有している。また、復号化部１１０ｂでもこの関係があることを前提に、復号化処理を実行する。

【００８１】上述したように、本発明の実施の形態に係る機器認証方法及び装置並びに認証システムは、第１の実施形態と同様な構成を設けた他、第１の実施形態と同様な効果が得られる他、秘密鍵Km とKr との間にｒ＝（ｍ＋ｃ）ｍｏｄ　ｎ（ｃは定数、１≦ｃ＜ｎ）という関係を設けたので、鍵Kr を送信側で繰り返し処理をすることなく特定することができる。このため制御信号１１２ｂが必要なくなり、また鍵Kr を特定するために第１の実施形態では最大ｎ回の計算が必要であったが、これを不要とすることができる。

【００８２】従って、本実施形態では鍵判定に要する計算量は、最大n^2 ＋ｎ回となり、高速処理に寄与する。なお、このような関係を持たせても秘密鍵を使用する限りセキュリティは保持される。

（発明の第4の実施の形態）本実施形態では、第1の実施形態における各鍵の関係を以下のようにする。

【0083】まず、暗号化部106aで用いる秘密鍵Kiと暗号化部107aで用いる秘密鍵Kjとが等しい、すなわちKi＝Kjであり、かつ復号化部108bおよび復号化部109bで用いた復号鍵Km（すなわち暗号化部108a及び暗号化部109aで用いる暗号鍵Km）と、暗号化部110aで用いる暗号鍵Krとが等しい、すなわちKm＝Krであるとする。なお、各暗号化部及び復号化部での処理はこの関係が前提とされる。

【0084】上述したように、本発明の実施の形態に係る機器認証方法及び装置並びに認証システムは、第1の実施形態と同様な構成を設けた他、Ki＝Kjかつ Km＝Krとしたので、第1の実施形態と同様な効果が得られる他、第2の実施形態同様にKaとKbそれぞれについて最大n回ずつの復号処理を不要とできる。また復号化部109bで用いる復号鍵Kmと復号化部110aで用いる暗号鍵Krとが等しいため、第3の実施形態と同様に、制御信号112bを不要とできる。

【0085】したがって、比較部111bで一致しなければ相互認証失敗として認証処理を終了してしまってよい。この場合の鍵判定に要する全計算量は最大n＋n＝2n回となる。

（発明の第5の実施の形態）図4は本発明の第5の実施形態の相互認証を行う部分の機能構成及び処理の流れの一例を示す図であり、図2と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0086】本実施形態では、受信側102に暗号化部113aが設けられ、送信側101に復号化部113bが設けられる他、第1の実施形態と同様に構成されている。暗号化部113aは、暗号化部107aで暗号化されたEKj（XOR（Kj，r1））を暗号鍵Kjを用いてさらに暗号化するものである。

【0087】この結果、EKj（EKj（XOR（Kj，r1））が受信側102から送信側101へ伝送されることになる。一方、復号化部113bは、このEKj（EKj（XOR（Kj，r1））を復号鍵Kbを用いて復号化し、その結果を復号化部107bに引き渡すものである。

【0088】本実施形態ではこのように構成されているので、暗号化部113aにて更なる暗号化がかけられ、また、この暗号化に対応して復号化部113bによる復号化がなされる。なお、暗号化部113aまでの処理及び復号化部107b以降の処理は第1の実施形態の場合と同様である。

【0089】上述したように、本発明の実施の形態に係る機器認証方法及び装置並びに認証システムは、第1の実施形態と同様な構成を設けた他、受信側102に暗号化部113a、送信側101に復号化部113bを設けて、受信側102から送出する認証用の情報について複数回の暗号化をかけるようにしたので、第1の実施形態と同様な効果が得られる他、より一層暗号解読を困難にし、伝送路上での暗号解読攻撃を防止することができる。

【0090】なお、本実施形態では、XOR（Kj，r1）について2回の暗号化を行うものとしているが、さらに多数回の暗号化を行うようにしてもよい。また、暗号化部106aの出力後にKiによる暗号化部を設けてKiの暗号化を複数回施すようにしてもよい。なお、これらの場合、送信側101には対応する復号化部が設けられる。

（発明の第6の実施の形態）図5は本発明の第6の実施形態の相互認証を行う部分の機能構成及び処理の流れの一例を示す図であり、図2と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0091】本実施形態では、受信側102に暗号化部114aが設けられ、送信側101に復号化部114bが設けられる他、第1の実施形態と同様に構成されている。復号化部114bは、復号化部108bで復号化（暗号化）されたDKm（XOR（Km，r2））を復号鍵Kmを用いてさらに復号化するものである。

【0092】この結果、DKm（DKm（XOR（Km，r2））が送信側101から受信側102へ伝送されることになる。一方、暗号化部114aは、このDKm（DKm（XOR（Km，r2））を暗号鍵Kaを用いて暗号化（復号化）し、その結果を暗号化部108aに引き渡すものである。

【0093】本実施形態ではこのように構成されているので、復号化部114bにて更なる復号化（暗号化）がかけられ、また、この復号化に対応して暗号化部114aによる暗号化（復号化）がなされる。なお、復号化部114bまでの処理及び暗号化部108a以降の処理は第1の実施形態の場合と同様である。

【0094】上述したように、本発明の実施の形態に係る機器認証方法及び装置並びに認証システムは、第1の実施形態と同様な構成を設けた他、受信側102に暗号化部114a、送信側101に復号化部114bを設けて、送信側101から送出する認証用の情報について複数回の復号化（暗号化）をかけるようにしたので、第1の実施形態と同様な効果が得られる他、より一層暗号解読を困難にし、伝送路上での暗号解読攻撃を防止することができる。

【0095】なお、本実施形態では、XOR（Km，r2）について2回の復号化を行うものとしているが、さらに多数回の復号化を行うようにしてもよい。なお、この場合、受信側102には対応する暗号化部が設けられる。

（発明の第7の実施の形態）図6は本発明の第7の実施

形態の相互認証を行う部分の機能構成及び処理の流れの一例を示す図であり、図2と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0096】本実施形態では、受信側102に暗号化部115aが設けられ、送信側101に復号化部115bが設けられる他、第1の実施形態と同様に構成されている。暗号化部115aは、暗号化部110aで暗号化されたEKr（r2）を暗号鍵Krを用いてさらに暗号化するものである。

【0097】この結果、EKr（EKr（r2））が受信側102から送信側101へ伝送されることになる。一方、復号化部115bは、このEKr（EKr（r2））を復号鍵Kbを用いて復号化し、その結果を復号化部110bに引き渡すものである。

【0098】本実施形態ではこのように構成されているので、暗号化部115aにて更なる暗号化がかけられ、また、この暗号化に対応して復号化部115bによる復号化がなされる。なお、暗号化部115aまでの処理及び復号化部110b以降の処理は第1の実施形態の場合と同様である。

【0099】上述したように、本発明の実施の形態に係る機器認証方法及び装置並びに認証システムは、第1の実施形態と同様な構成を設けた他、受信側102に暗号化部115a、送信側101に復号化部115bを設けて、受信側102から送出する2回目の認証用の情報について複数回の暗号化をかけるようにしたので、第1の実施形態と同様な効果が得られる他、より一層暗号解読を困難にし、伝送路上での暗号解読攻撃を防止することができる。

【0100】なお、本実施形態では、乱数r2について2回の暗号化を行うものとしているが、さらに多数回の暗号化を行うようにしてもよい。なお、この場合、送信側101には対応する復号化部が設けられる。

（発明の第8の実施の形態）第1～第7の実施形態においては、図1に示すように、送信側101及び受信側102としてDVD－ROMドライブ1及びMPEGデコータ2を用いた場合について説明した。しかしながら、本発明の適用はこのような場合に限られるものではない。そこで、本実施形態では、本発明が適用される機器の組み合わせ例について説明する。

【0101】図7は本発明の第8の実施の形態について説明する図である。まず、同図（a）は、図1の場合と同様に機器間が1394ケーブル206によって接続される場合を示す例である。この場合、パーソナルコンピュータ201、DVDドライブ202、D－VCR203、ハードディスク204、光磁気ディスクドライブ205夫々には、第1～7の実施形態の1394チップ4又は5が搭載され、各機器間で通信が行われる際には、第1～7の実施形態で説明したと同様な相互認証がなされる。

【0102】次に、同図（b）は、公衆回線211にLAN#1，#2，#3が接続され、また、モデム212、214を介して夫々パーソナルコンピュータ213、ワークステーション215が接続され、ネットワークが形成される場合である。

【0103】このようなLAN#1，#2，#3、また、パーソナルコンピュータ213、ワークステーション215には、第1～7の実施形態の1394チップ4又は5が搭載され、各機器間で公衆回線211を介したネットワーク通信が行われる際には、第1～7の実施形態で説明したと同様な相互認証がなされる。

【0104】次に、同図（c）は、パーソナルコンピュータ211内で、その内部機器での通信が行われる場合である。このパーソナルコンピュータ211においては、CPUバス222にCPU223、内部ハードディスク224、メモリ225、ビデオメモリ227を有するビデオボード226が接続されている。

【0105】これらの接続機器のうち、例えば内部ハードディスク224やビデオボード226には、第1～7の実施形態の1394チップ4又は5が搭載され、各機器間でCPUバス222を介したデータ伝送が行われる際には、第1～7の実施形態で説明したと同様な相互認証がなされる。

【0106】このように本発明の実施の形態では、本発明にかかる機器認証方法及び装置並びに認証システムが種々の機器において、また種々の場合において適用されるものであることを説明した。

【0107】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。例えば上記各実施形態は、適宜に組み合わせて実施することができる。

【0108】また、上記各実施形態はIEEE1394規格を用いた場合で説明したが、本発明の適用対象はこのような規格に限定されるものでなく、種々の場合に適用可能である。

【0109】

【発明の効果】以上詳記したように本発明によれば、共通鍵を複数個使用し、かつ鍵及び乱数を用いた暗号化あるいは復号化の演算を施してから認証用情報を送出するようにしたので、第三者の攻撃による秘密鍵の推定を一層困難にし、相手が正当な機器であるかを安全かつ確実に認証できる機器認証方法及び装置並びに認証システムを提供することができる。

【図面の簡単な説明】

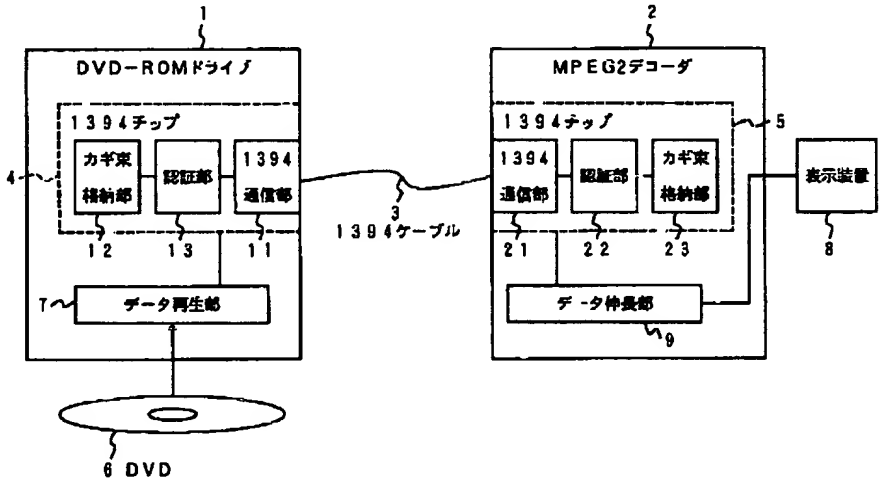
【図1】本発明の第1の実施の形態に係る機器認証方法を適用する機器の構成例を示すブロック図。

【図2】同実施形態の相互認証を行う部分の機能構成及び処理の流れの一例を示す図。

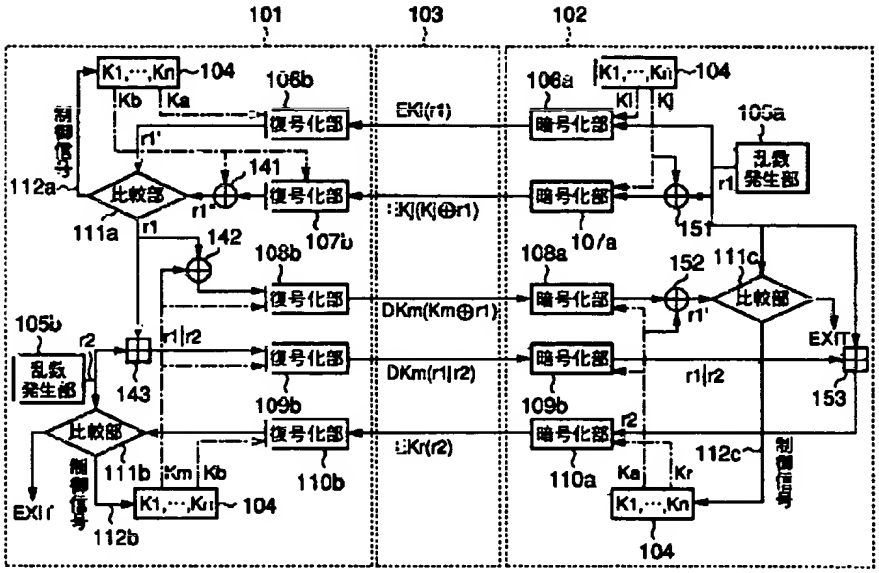
【図3】同実施形態の認証動作例を示す流れ図。

【図4】本発明の第5の実施形態の相互認証を行う部分の機能構成及び処理の流れの一例を示す図
【図5】本発明の第6の実施形態の相互認証を行う部分の機能構成及び処理の流れの一例を示す図。
【図6】本発明の第7の実施形態の相互認証を行う部分の機能構成及び処理の流れの一例を示す図。
【図7】本発明の第8の実施の形態について説明する図。
【符号の説明】
1…DVD－ROMドライブ
2…MPEG2デコーダ2
3…1394ケーブル
4，5…1394チップ
6…DVD
7…データ再生部
9…データ伸張部
11，21…1394通信部
12，22…鍵束格納部
13，23…認証部
101…送信側
102…受信側
103…ネットワーク
104…共通鍵束
105a，105b…乱数発生部
106a，107a，108a，109a，110a，113a，114a，115a…暗号化部
106b，107b，108b，109b，110b，113b，114b，115b…復号化部
111a，111b，111c…比較部
112a，112b，112c…制御信号
141，142…排他的論理和演算部
143…連接演算部
151，152…排他的論理和演算部
153…連接演算部

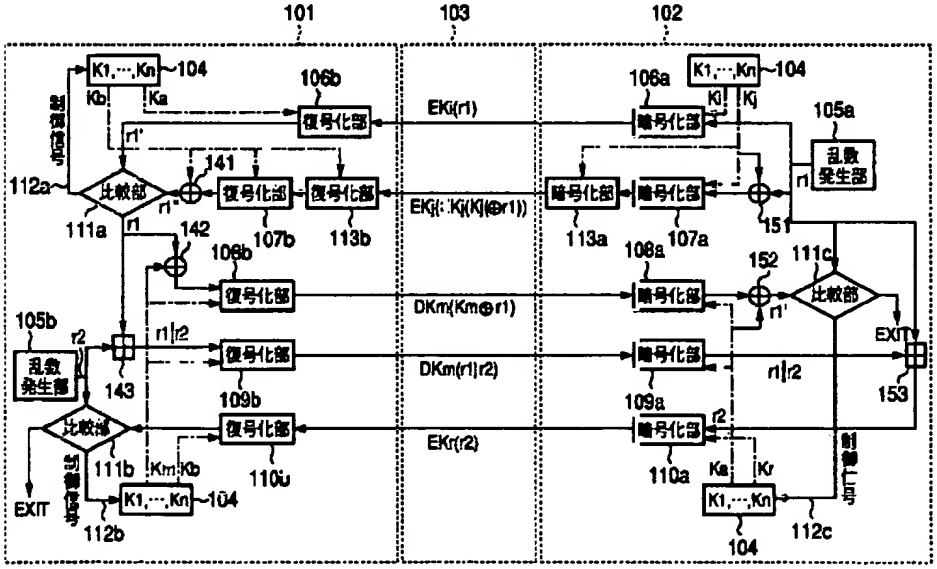
【図1】



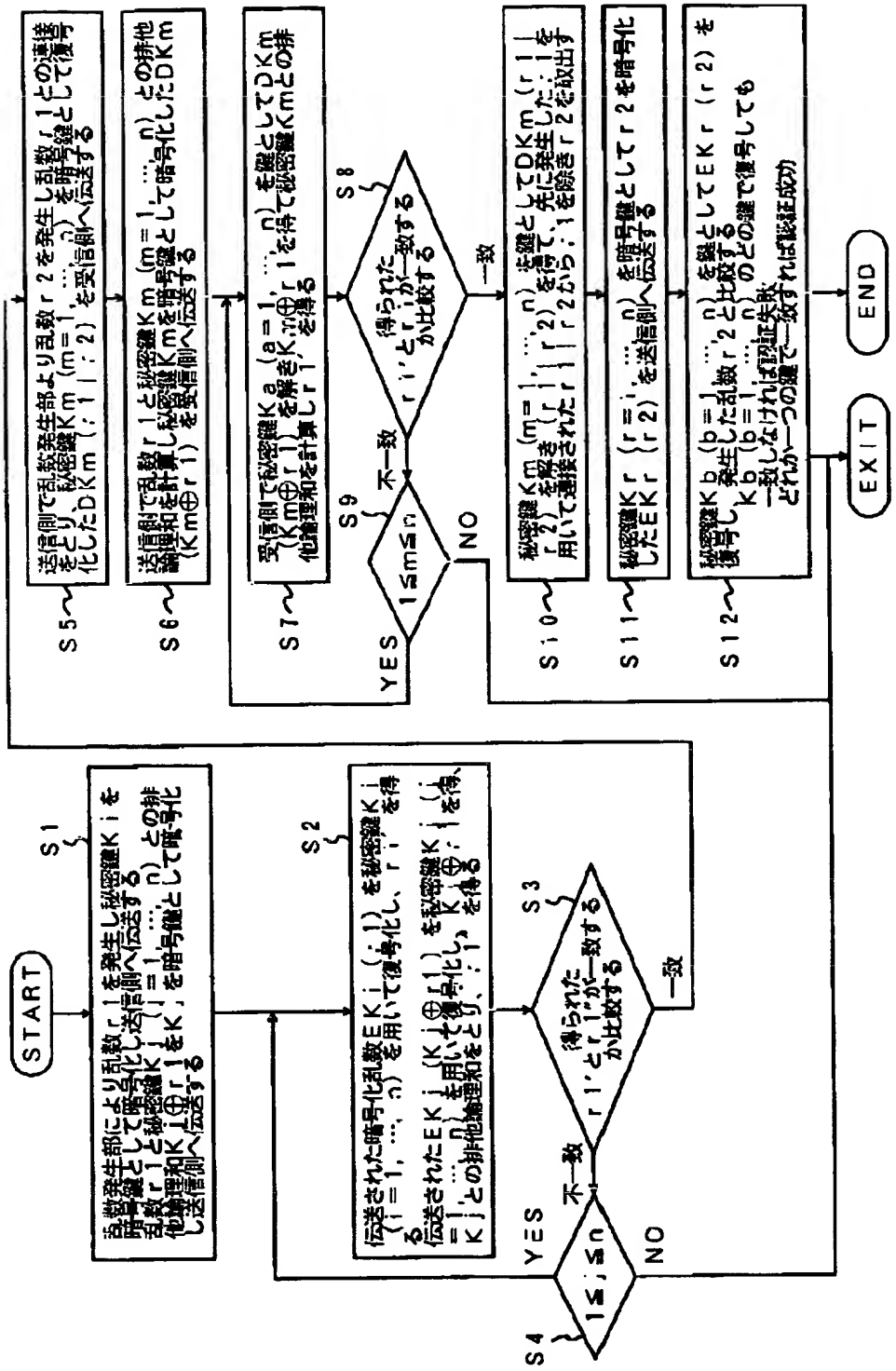
【図2】


101
103
102
K1,…,Kn
104
Kb
Ka
106b
復号化部
EKi(r1)
106a
Ki
Kj
暗号化部
105a
乱数発生部
r1
制御信号
112a
比較部
r1'
141
111a
107b
:Kj(Kj⊕r1)
107a
151
142
108b
DKm(Km⊕r1)
108a
152
111c
105b
r2
r1|r2
143
DKm(r1|r2)
EXIT
153
109b
110b
:Kr(r2)
110a
Km
Kr
112c
EXIT
112b

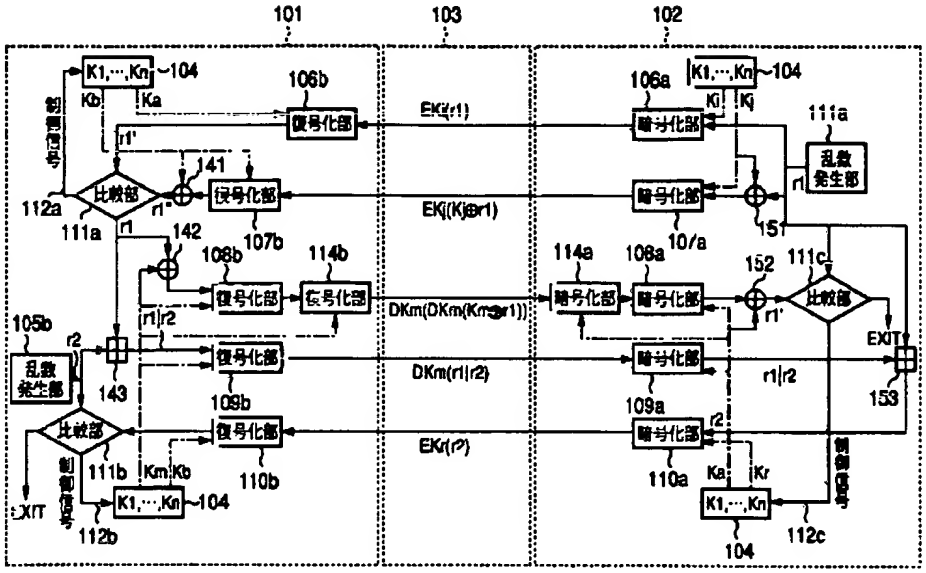
【図4】


101
103
102
K1,…,Kn
104
Kb
Ka
106b
復号化部
EKi(r1)
106a
Ki
Kj
暗号化部
105a
乱数発生部
r1
制御信号
112a
比較部
r1'
141
111a
107b
113b
EKi(:Kj(Kj⊕r1))
113a
107a
151
142
108b
DKm(Km⊕r1)
108a
152
111c
105b
r2
r1|r2
143
DKm(r1|r2)
EXIT
153
109b
109a
110b
EKr(r2)
110a
Km
Kr
112c
EXIT
112b

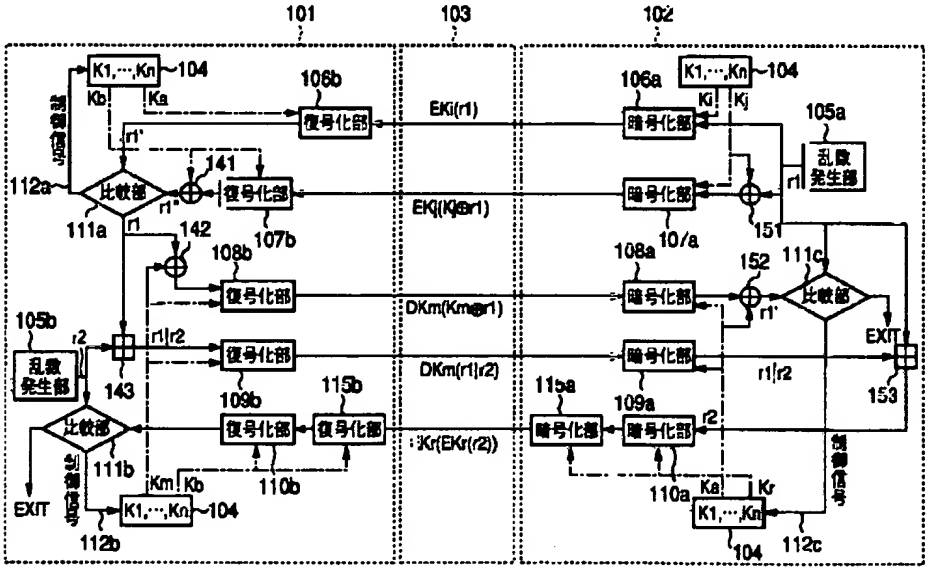
【図3】



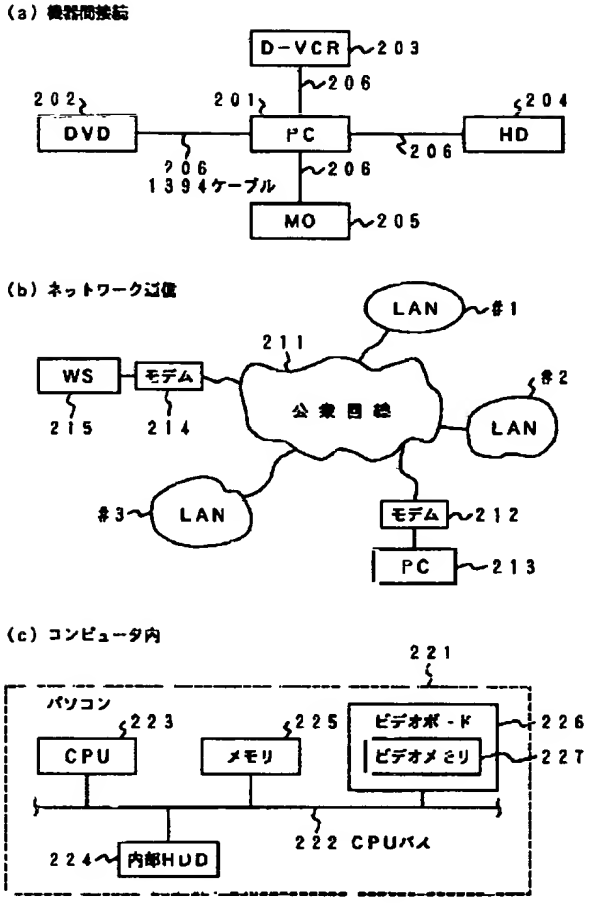
【図5】


101
103
102
K1,…,Kn
104
Kb
Ka
106b
復号化部
EKr(r1)
106a
暗号化部
Ki
Kj
111a
乱数発生部
r1
141
比較部
112a
111a
r1'
r1
142
107b
EKj(KjBr1)
151
108b
114b
114a
108a
152
111c
DKm(DKm(KmBr1))
105b
r2
r1|r2
DKm(r1|r2)
EXIT
153
143
109b
109a
EKr(r2)
110b
110a
Km
Ka
Kr
112b
112c
104

【図6】


101
103
102
K1,…,Kn
104
Kb
Ka
106b
復号化部
EKi(r1)
106a
暗号化部
Ki
Kj
105a
乱数発生部
r1
141
比較部
112a
111a
r1'
r1
142
107b
EKj(KjBr1)
151
108b
108a
152
111c
DKm(KmBr1)
105b
r2
r1|r2
DKm(r1|r2)
EXIT
153
143
109b
115b
109a
:Kr(EKr(r2))
110b
110a
Km
Kb
Ka
Kr
112b
112c
104

【図7】


(a) 機器間接続
D-VCR
203
206
202
201
204
DVD
PC
HD
206
206
206
1394ケーブル
MO
205
(b) ネットワーク通信
LAN
#1
211
WS
モデム
#2
公衆回線
215
214
LAN
#3
LAN
モデム
212
PC
213
(c) コンピュータ内
221
パソコン
223
225
ビデオボード
226
CPU
メモリ
ビデオメモリ
227
222 CPUバス
224
内部HDD